RICO Title 47

FOX 00383

A hacking blow

The private civil damages and equitable relief amendments of the federal Computer Fraud and Abuse Act are powerful litigation weapons, writes Joel D. Covelman

The case of computer-science graduate student Robert Morris, convicted for unleashing his "worm" computer program that shut down large segments of the Internet, is the most widely known criminal prosecution under the federal Computer Fraud and Abuse Act (CFAA). See *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991). This prosecution exposed weaknesses in the statute, prompting a legislative amendment in 1994. 18 U.S.C. Section 1030.

Although the private civil damages and equitable relief provisions added then have been largely ignored by civil lawyers for technology developers and end users, these new civil remedies can be powerful weapons against computer abuses, such as financial and consumer credit fraud, computer hacking, sabotage by disgruntled present or former employees, competitor spying, medical computer tampering and even overreaching by suppliers of computer systems or software.

Paragraph (a)(2) prohibits simple unauthorized snooping, or hacking, of a financial institution's computer. Access that exceeds the scope of authorization or wholly unauthorized access to computerized consumer credit records, or to a financial institution's other computer files, is also prohibited. A consumer or business whose records have been improperly accessed, as well as the financial institution that maintains the records, may bring suit under the statue for damages and injunctive or other equitable relief.

***Joel D. Covelman**, a Costa Mesa, Calif., attorney, represents technology developers and users in litigation, arbitration and mediation.*

Commission of fraud using a "federal interest computer" is prohibited. CFAA Paragraph (a)(4). The definition of a federal interest computer includes a computer used exclusively by a financial institution, or if shared with others, the fraud perpetrated must also impair the financial institutions' operations performed on the computer. Section (e)(2). The definition also describes a federal interest computer as one of two or more computers used in connection with the fraud, at least one of which is located in a different state.

A fraudulent scheme carried out between computers in different states, connected via modems, whether the target computer is used by a financial institution or not, is thus prohibited by Paragraph (a)(4). It is less obvious, however, that the telephone switches making the modem connections are themselves special-purpose computers. Even when the malefactor's computer and the victim's computer are located in the same state, if the modem connection is made via a telephone switch located in another state, a Paragraph (a)(4) violation has occurred.

Paragraph (a)(5) is divided into subsections (A) and (B). Each prohibits the spreading of harmful software code or data, but with differing scienter requirements. Subsection (A) prohibits knowing dissemination of harmful software or data with the intent to cause harm to a computer, network or data, or with the intent to deny access to a computer, network or data. Subsection (B) prohibits knowing dissemination of harmful software or data in reckless disregard of the harm it may cause.

Each subsection, under the heading (II)(aa), requires that transmission of the offending software or data must have caused at least $1,000 in damage. But each subsection contains an exception to this minimum damage requirement for medical computers. When there has been impairment, or the threat of impairment, of medical diagnosis or treatment, no minimum monetary damage need be shown.

Paragraph (a)(5) speaks of "transmission" of harmful software or data to another computer or network "through means of a computer used in interstate commerce or communications," suggesting that the offense is limited to the spread of damaging data or code from computer to computer via telephone wires or radio transmissions. Almost any computer with a modem used to dial up an out-of-state data service, bulletin board or e-mail server is one used in interstate communications or commerce.

But the legislative history of the 1994 amendment shows that Paragraph (a)(5) was intended to reach the spread of viruses, time bombs and other harmful software via infected computer disks, created on a computer used in interstate commerce or communications, and then physically passed to one or more unsuspecting victims. See 136 Cong.Rec. S18235 (daily ed. Oct. 25, 1990), statement of Sen. Humphrey of New Hampshire) ("[A] destructive computer virus can be transmitted — either through electronic means or by the physical transfer of an infected disk to a remote computer system even though the originator of the virus never gained personal access to that system. ... S2476 closes this potential loophole in existing law.").

Today software vendors and developers routinely include "expiration" or "deactivation" code in the products they distribute. Usually, the fact that the software will cease to function, and the data it generated will cease to be accessible on a predetermined date, is fully disclosed to the customer at the outset.

For example, a software publisher may offer a 30-day evaluation sample of its product, which may be obtained on disk or by downloading from an Internet site. If the user wishes to continue to use the product after the evaluation period, then the purchase price must be paid, and the vendor will either send a new disk or deactivate the expiration code in the evaluation copy via modem. This disclosed-at-the-outset disabling of software is not prohibited by the CFAA. See 140 Cong.Rec. S12313 (daily ed. Aug. 23, 1994, statement of Senator Leahy of Vermont) ("[I]t is not the intent of this legislation to criminalize use of disabling codes when their use is pursuant to a lawful licensing agreement that specifies the conditions for

See COVELMAN, page 22

ADW

FOX 00384

COVELMAN

Continued from page 21

reentry or software disablement.").

On the other hand, computer-system vendors or software developers sometimes bury disabling mechanisms in a customer's software as leverage to ensure that the purchase price or lease payment is made by the customer. In one publicized case, *Werner, Zuroff, Slotnick, Stern & Askenazy v. Lewis*, 588 N.Y.S.2d 960 (N.Y. Civ. Ct. 1992), a consultant hid disabling code in a law firm's computers to ensure that the firm would pay for later repair service and maintenance. This kind of undisclosed deactivation device, whether factory-installed on the computer system, hidden in software to be installed by the customer upon delivery or added later by the vendor in the face of a deteriorating relationship with the customer, is prohibited by Paragraph (a)(5).

Paragraph (a)(6) prohibits trafficking in computer passwords with the intent to defraud, when such trafficking affects interstate or foreign commerce. Manufacturers whose trade secrets are stolen from their computers by industrial spies may recover damages and obtain injunctive relief if a stolen password was obtained to gain access to these business secrets.

Since the statute requires only that there be an effect upon interstate commerce, not interstate trafficking in passwords, the dissemination of computer passwords occurring entirely within a single state can still constitute a violation of Paragraph (a)(6). Furthermore, the statute speaks of passwords, or "similar information," which could include reproductions of fingerprints or voice recordings used for identification of permitted computer users.

The CFAA defines a computer as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to ... such device." The only devices specifically excluded from the statute's definition of a computer are an automated typewriter or typesetter and a portable hand-held calculator.

Devices as varied as telephone switches, the new generation of laptop and palmtop computers and hand-held personal organizers fit within the CFAA's definition of a computer. Even the electronic gasoline pump — which verifies magnetically encoded credit card payment information, calculates the gallons and price of fuel pumped and transmits the information to the oil company's billing computer is a computer as defined by the CFAA.

Paragraph (g) contains the CFAA's civil remedies provisions. A victim of the statute's enumerated computer abuses is granted the right to bring an action for compensatory damages, limited to economic losses, except in the case of tampering with medical computers. The statute authorizes "[a]ny person who suffers damage or loss by reason of a violation of the section, other than a violation of subsection (a)(5)(B), [to] maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations of any subsection other than subsections (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb) are limited to economic damages."

Subparagraph (a)(5)(B) is the provision that prohibits the spreading of harmful software or data with reckless disregard for the harm that may be caused. This entire subparagraph appears at first to be carved out of the civil remedies provision. But subsection (a)(5)(B)(ii)(II)(bb) is a sub-subsection of (a)(5)(B), prohibiting tampering with medical computers. Under the second sentence of Paragraph (g), a violation of this sub-subsection allows a victim to recover damages apparently broader than economic losses.

Curiously, civil injunction or other equitable relief does not appear to be available at all to victims of reckless transmission of harmful software or data to any computer. Why the legislative prerogative was exercised to criminalize reckless tampering with all computers, while denying all civil injunctive or equitable relief to the victims, including the victims of reckless tampering with medical computers, is not clear from the legislative history. This may be a drafting oversight rather than a conscious omission.

Although Paragraph (g) is confusingly worded with respect to what compensatory damages may be recovered by a victim of reckless or intentional harm to a medical computer, by negative implication and legislative history, it appears that general damages for pain and suffering are available in addition to economic damages. See S. Rep. No. 544, 101st Cong., 2nd Sess. at 10 (Oct. 19, 1990) ("Damages are limited to economic damages, except for violations of the medical records section, when pain and suffering damages would be permitted.").

But it should also be the case that other damages proximately caused, such as for loss of consortium, disfigurement or loss of enjoyment of life should be recoverable.

Furthermore, while the obvious focus of the CFAA's provisions dealing with medical-computer tampering is on injury to a patient whose diagnosis or treatment has been impaired, a manufacturer of medical computers whose products are sabotaged by an employee, or whose bid price is undercut by a spying competitor, or a health care provider whose imaging or surgical computer is likewise sabotaged, may have economic damages from lost sales or loss of use of the computer equipment and related facilities. These losses are recoverable under the CFAA provisions applicable to medical and nonmedical computers alike.

The CFAA authorizes civil injunctive relief for violations of many of its provisions. In the case of spreading harmful software or data, such as delayed-acting viruses, time-delayed deactivation devices or logic bombs that destroy data or deactivate a computer upon a predetermined occurrence, a mandatory injunction may be required. It may be necessary to require the defendant to furnish software to deactivate previously implanted harmful software or a new program that is free of the virus, time bomb or logic bomb. The statute's specific recognition of the right to obtain injunctive relief should help to overcome any judicial reluctance to grant a mandatory injunction.

The CFAA's authorization of other equitable relief should not be overlooked. For embezzlement or other theft, an accounting or a constructive trust may be a highly effective remedy.

The limitations period for civil actions, found in Paragraph (g), is two years from the date of the act that is the subject of the suit, or in the alternative, two years from the date the harm was discovered. The alternative limitations period can be useful for embezzlement, or other theft, where the crime is camouflaged by further manipulation of computer records.